

UNITED STATES DISTRICT FOR THE
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN STUART,

Defendant.

21-CR-07-LJV-JJM

REPLY MEMORANDUM

The government argues in its response brief that: (1) there is nothing new in the information presented in Mr. Stuart's supplemental brief; (2) there is no expectation of privacy in IP addresses even when the user takes affirmative steps to keep that information private; and (3) the search warrant is saved by good faith so long as the warrant affiant had no knowledge of the unlawful antecedent Fourth Amendment violation. For the reasons that follow, this Court should not credit any of these assertions; it should instead order an evidentiary hearing.

1. Information establishing coordination, and more.

The government suggests in its response that information presented in the supplemental brief is untimely. But the defense is now able to present this information only after dogged efforts to obtain it, and against government efforts resisting its disclosure. The defense filed a motion to compel in July of 2022 and filed a motion for discovery in October of 2021 seeking information akin to that presented in the supplemental briefing. Both those motions were resisted by the government, and it provided only a few documents relative to the requests and demands. It also provided a letter purporting to provide a second-hand account from the government's perspective of what had occurred leading to the execution of the search warrant. The government

should not be permitted to sit on allegedly unrecoverable evidence and then rely on that lack of disclosure to claim that Mr. Stuart did not timely present his case. *See, e.g., United States v. Budziak*, 697 F.3d 1105, 1112 (9th Cir. 2012) (“In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless.”).

Critically, the information gleaned as a result of the FOIA request shows that prosecutors in the U.S. Attorney’s Office in Massachusetts were working on an affidavit in support of a search warrant *before* the government claims to have received the lucky tip. In emails in July of 2019 – months before the “tip” in either August or November of 2019¹ – agents and attorneys at the U.S. Attorneys office for the District of Massachusetts (“USAMA”), were sending emails to each other with the subject line “affidavit so far.” (attached as Exhibit A, highlighting added). Later, the subject line is changed to “Tor OP go by.” (*Id.*) Further emails were sent in September of 2019 discussing “website A” and “B.” (*Id.*) Other emails contains an attachment entitled “[Country 1]² storage devices affidavit.” (*Id.*) These emails, in short, contain attachments for residential search warrants in the United States before the government claimed to have known of any U.S.-based IP addresses associated with the site. This is far from immaterial, as the government seems to suggest in its response. It is devastating to the claim that the U.S. government received a tip and only then began seeking out U.S. IP addresses associated with the site. They were drafting warrants and including descriptions of the websites before the “tip” was even received.

¹ Hockwater writes in the search warrant affidavit that the tip was received in August of 2019. But documents from the FBI to the Buffalo Field Office that attempt to explain the investigation to the Buffalo office provide that the tip was received in November of 2019. (This internal FBI document is subject to a protective order and can be provided to the Court under separate cover if necessary). Such discrepancies in the government’s own documents further solidify the need for a hearing.

² The true name of the country is omitted pursuant to a protective order in this case.

Finally, the government has no retort to the fact that Agent Squire was so involved in this investigation that he received an award from the FLA for his work. Once again, United States law enforcement agents do not receive awards for simply receiving “tips.” A hearing is absolutely necessary to determine the full level of United States involvement, and the manner and means in which U.S. citizens’ hidden IP addresses were uncovered.

2. Tor users have a legitimate expectation of privacy in their IP addresses.

Nothing in the government’s response should lead these to Court to conclude that a Tor user does not maintain a reasonable expectation of privacy in his IP address. The government cites the same district court cases identified in Mr. Stuart’s brief. Those are not compelling for the reasons already outlined.

Additionally, this Court should not credit the district court’s misguided suggestion in *United States v. Matish* that the expectation of privacy is eliminated simply because the first node in the TOR browser’s path must know the IP address. 193 F. Supp. 3d 585 (E.D. Va. 2016). In the seminal case on the third-party doctrine, *Smith v. Maryland*, the Supreme Court reasoned that, “when [the defendant] used his phone, [he] voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, [the defendant] assumed the risk that the company would reveal to police the numbers he dialed.” 442 U.S. 735, 744 (1979). This assumption-of-risk rationale, applied in the context of a pen register in *Smith*, was also applied earlier in the case of bank records in *United States v. Miller*. There, the Supreme Court held, “The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. 425 U.S. 435, 443 (1976).

The TOR user, however, assumes no such risk, as the IP address is not stored and the entire system is specifically designed to scrub and obfuscate the true IP address. Unlike a phone or bank record, this information cannot be turned over to the police absent the sort of state sponsored hacking that it appears occurred here. Moreover, as argued in the supplemental brief, *Carpenter* calls into question the continued validity of the third-party doctrine in the context of data that can reveal the most intimate details of persons life, especially when that person has done nothing more than access the internet or a cell phone, necessary components of modern life.

3. The head-in-the-sand officer, and those placing him in that position, were not operating in good faith.

In a ruling several months ago before much of this information came to light, this Court wrote that “Like Judge McCarthy, this Court wonders why the identity of the FLA (or at least the country of origin) could not have been revealed in Hockwater’s affidavit.” (Docket No. 44). It is clear now why this information was hidden from this court. FOIA documents suggest that the USAMA assisted the FBI and HSI in constructing a “boilerplate” affidavit that hid the true nature of the investigation from the issuing-magistrate judges. This is bad faith, and points to a systemic, multi-agency effort to hide potential constitutional violations from the court – actions that are well suited for the deterrent effect of suppression.

The government continues to advocate for an approach that would provide cover to unsanctionable police conduct. Under its philosophy, so long as the search-warrant applicant *himself* did not commit any Fourth Amendment violation, the warrant is valid. But it is not just TFO Hockwater that the suppression remedy is meant to deter, it is the law-enforcement team writ large. The defense has argued that, at a minimum, a hearing is necessary to determine

whether any Fourth Amendment violations occurred in the course of the investigation leading up to the application for the search warrant for Mr. Stuart's home. If one is established, the hypothetical fact that Hockwater was not involved provides no sanction to those who did commit the violations.

The cases cited by the government are not to the contrary. Tellingly, its Second Circuit cases stand only for the proposition that in rare circumstances, good faith *might* still apply if there were a Fourth Amendment violation before a search warrant. Typically, good faith does not apply in such situations. And in *McClain*, the Sixth Circuit found that an antecedent Fourth Amendment violation should not result in suppression because, although probable cause did not exist for the antecedent search, "we do not believe officers were objectively unreasonable in suspecting that criminal activity was occurring inside McClain's home, and we find no evidence that the officers knew they were violating the Fourth Amendment by performing a protective sweep of the home." *United States v. McClain*, 444 F.3d 556, 566 (6th Cir. 2005). The Court noted that a different agent applied for the warrant but emphasized that the warrant "affidavit fully disclosed to a neutral and detached magistrate the circumstances surrounding the initial warrantless search." *Id.* Indeed, the theme of all the government's cases is that the magistrate was fully informed of the previous unlawful investigation and still issued a warrant. That is a world apart from what occurred here, where the magistrate was intentionally kept in the dark. No information whatsoever was provided on anything before the magical tip arrived, including the circumstances of the investigation, that the U.S. had been involved for years, or that the U.S. spearheaded the investigation by uncovering the server in the first FLA. Such information might have prompted the magistrate to ask questions about just how it was the IP addresses were uncovered.

If, after a hearing, this Court concludes that a Fourth Amendment violation occurred, it should have no trouble further concluding that the magistrate was not fully informed about the nature of that violation.

For all these reasons, this Court should order an evidentiary hearing.

Dated: Buffalo, New York
January 9, 2024

Respectfully submitted,

/s/ Jeffrey T. Bagley

Jeffrey T. Bagley

jeffrey_bagley@fd.org

Assistant Federal Public Defenders

Federal Public Defender's Office

300 Pearl Street, Suite 200

Buffalo, New York 14202

(716) 551-3341

Counsel for John Stuart